



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/277,335	03/26/1999	DEAN A. KLEIN	MPATENT.053A	3400

20995 7590 04/02/2004

KNOBBE MARTENS OLSON & BEAR LLP  
2040 MAIN STREET  
FOURTEENTH FLOOR  
IRVINE, CA 92614

EXAMINER
----------

HAMILTON, MONPLAISIR G

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 04/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/277,335

Applicant(s)

KLEIN, DEAN A.

Examiner

Monplaisir G Hamilton

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 26 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-10 and 12-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 and 12-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 23.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/19/03 has been entered.

The communication filed on 12/19/03 amended Claims 1, 5 and 7. Claims 1-10 and 12-14 remain for examination.

### ***Information Disclosure Statement***

2. The information disclosure statement (IDS) submitted on 3/18/04 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

### ***Response to Arguments***

3. Applicant's arguments with respect to Claims 1-10 and 12-14 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 7-8 are rejected under 35 U.S.C. 102(a) as being anticipated by US 5818939 issued to Davis, herein referred to as Davis.

Referring to Claim 7:

Davis discloses a computer system comprising a processor and encryption hardware and at least one data storage device, a method of data storage comprising;

transmitting data from the processor in the computer system to encryption hardware in the computer system (col 4, lines 5-35); and

encrypting and decrypting, in the encryption hardware, user generated data with an encryption process, wherein the encryption process retrieves information that is stored in a nonerasable memory in said computer system during manufacture of said computer system (col 5, lines 20-45).

Art Unit: 2135

Referring to Claim 8:

Davis discloses the limitations of Claim 7 above. Davis further discloses said information is permanently associated with said host computing logic (col 5, lines 25-40).

Art Unit: 2135

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 3-6 and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6032257 issued to Olarig et al, herein referred to as Olarig in view of US 5513262 issued to van Rumpt et al, herein referred to as Harm.

Referring to Claims 1 and 5:

Olarig disclose in a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer (col 5, lines 25-65; col 8, lines 10-15);  
retrieving the identification code from the memory in said personal computer (col 9, lines 1-10);  
generating a cryptographic key derived at least in part from said identification code (col 9, lines 25-35);

Art Unit: 2135

Olarig does not explicitly disclose “encrypting and decrypting data, for storage on and retrieval from one of said data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware.”

Harm discloses encrypting and decrypting data, for storage on and retrieval from one of said data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware (col 3, lines 10-20; col 2, lines 40-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art it would have been obvious to one of ordinary skill in the art to include generate a key based partially on a (manufacturer id or code). One of ordinary skill in the art would have been motivated to do this because it would enable the manufacturer to control what devices can read the data stored on the storage media (Olarig: col 4, lines 35-60), preventing the theft of confidential information.

Referring to Claim 3:

Olarig in view of Harm discloses the limitations of Claim 1 above. Olarig further discloses said retrieving is performed without intervention by a host processor (col 9, lines 4-10).

Art Unit: 2135

Referring to Claim 4:

Olarig in view of Harm discloses the limitations of Claim 3 above. Olarig further discloses verifying said key, wherein said verifying occurs without intervention of said host processor (col 9, lines 15-25).

Referring to Claim 6:

Olarig in view of Harm discloses the limitations of Claim 5 above. Harm further discloses said act of connecting comprises routing a serial data bus from said memory integrated circuit to said logic circuit (col 2, lines 1-25).

Referring to Claim 13:

Olarig in view of Harm discloses the limitations of Claim 1 above. Harm further discloses encrypting data for storage is performed on an encrypting device that is positioned in a data path between a central processing unit and the data storage medium (Fig. 1; col 2, lines 5-20).

Referring to Claim 14:

Olarig in view of Harm discloses the limitations of Claim 1 above. Harm further discloses wherein all data that is transmitted to the data storage media is encrypted (col 3, lines 5-20).



Art Unit: 2135

6. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over US 6032257 issued to Olarig et al, herein referred to as Olarig in view of US 5513262 issued to van Rumpt et al, herein referred to as Harm further in view of 5343525 issued to Hung et al, herein referred to as Hung.

Referring to Claim 2:

Olarig in view of Harm discloses the limitations of Claim 1 above.

Olarig in view of Harm do not explicitly disclose “retrieving information from a memory location; and disabling encryption of data routed to one of said data storage media in response to said retrieved information.”

Hung discloses retrieving information from a memory location; and disabling encryption of data routed to one of said data storage media in response to said retrieved information (col 2; lines 50-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Olarig in view of Harm such that encryption is disabled in response to retrieved information. One of ordinary skill in the art would have been motivated to do this because it would allow a administrator to decide whether to implement the security featured of the storage device (Hung: col 1, lines 55-65 and col 2, lines 55-65).

Art Unit: 2135

7. Claims 9-10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5818939 issued to Davis, herein referred to as Davis further in view of 5231662 issued to van Rumpt et al, herein referred to as Rumpt.

Referring to Claim 9:

Davis discloses the limitations of Claim 7 above.

Davis does not explicitly disclose "said information comprises a multibit identification code".

Rumpt discloses said information comprises a multibit identification code (col 3, lines 15-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Davis such that a multibit id code is used. One of ordinary skill in the art would have been motivated to do this because it would allow the encryption process to encrypt different sectors with different portions of the code (Rumpt: col 6, lines 10-25).

Referring to Claim 10:

Davis in view of Rumpt discloses the limitations of Claim 9 above. Rumpt further disclose deriving an encryption key at least in part from said identification code (col 6, lines 10-25).

Art Unit: 2135

Referring to Claim 12:

Davis discloses the limitations of Claim 7 above.

Davis does not explicitly disclose “defining said encryption process at least in part from user input to said computer system”.

Rumpt defining said encryption process at least in part from user input to said computer system (col 3, lines 15-45).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Davis such that the encryption process is defined as a function of a user input. One of ordinary skill in the art would have been motivated to do this because it would provide a further level of security (Rumpt: col 3, lines 20-35).

#### ***Prior Art***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 6343282 issued to Oshima, Mitsuaki et al. Oshima disclose a device for reading encrypted information recorded on an optical disk having first and second recording areas, the device can read disk identification information recorded in the second recording area, select a specific decipher key among multiple decipher keys, and decrypt encrypted information from the optical disk using both the disk identification information unique to that optical disk and the specific decipher key.

Art Unit: 2135

US 5212729 issued to Schafer, Randy J. Schafer discloses an apparatus and method for protecting data stored on a disk of a computer. The invention provides data access protection using a security software program, a hardware key, and a user password to permit access to the hard or floppy disk used in the computer. The program stores the hardware key code and password on the disk and encrypts disk partition data, and without using the correct hardware key and password, the partition data is unreadable. An encryption algorithm operates at all times and prevents unauthorized entry once the computer is turned off. A microcircuit key provides a unique stored code when energized, and a key connector is provided to use the key. The computer connector may also be adapted to permit coupling of an output device to the computer. Versions are disclosed for use with ports having bi-directional and unidirectional input and output lines.

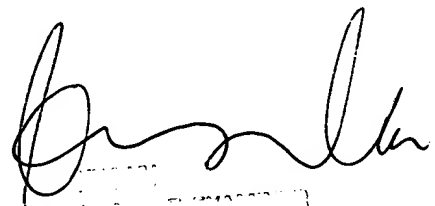
***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monplaisir G Hamilton whose telephone number is (703) 305-5116. The examiner can normally be reached on Monday - Friday (8:00 am - 4:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Monplaisir Hamilton



Monplaisir G. Hamilton  
Examiner